USCG TELECONFERENCING GUIDANCE

This Teleconferencing Guide will help you create a workflow using technology more efficiently for yourself as well as for the Coast Guard as a whole. Please refer to the most recent ALCOAST regarding teleworking options, categories, and information at https://www.uscg.mil/Coronavirus/

TELECONFERENCING CAPABILITIES:
The recommended DoD-approved methods of teleconferencing and collaboration are Defense Collaboration Services (DCS) https://conference.apps.mil/dashboard and milSuite https://login.milsuite.mil/ . These tools are secure, authorized, and available on the Internet for use outside of the Coast Guard network with a CAC reader. For further details, please refer to https://www.dcms.uscg.mil/Telework/ for the most updated list.

TELECONFERENCING EXCEPTIONS: If the DoD-approved teleconferencing and colloboration solutions do not provide the necessary capabilities to a unit commander, then Third-Party applications (apps), such as Zoom or Adobe Connect can be installed ONLY on personal and government mobile devices (smart phones and tablets) and are limited to "off network" use.

Third-party teleconferencing, videoconferencing, and collaboration apps are NOT authorized on CG Government Furnished Equipment (GFE) Standard Workstation Laptops. These off-network Third-party apps offer the capability for collaborating remotely while also not using and preserving Coast Guard's CGOne bandwidth. **However, these Third-party apps should be used as a last resort because they have known associated risks.** See the "Helpful Links" at the end of this document for further details. CGCYBER will continue to evaluate risks and put out information to advise users, while working with CG-6 to provide more secure collaboration alternatives that will allow us to migrate away from unsafe applications and ensure the protection of CG information and data.

USES FOR THIRD-PARTY TELECONFERENCING APPS:
Third-party apps are commercial video/web conferencing applications that can be utilized to discuss publicly releasable information, and to assist communications within the USCG community during the COVID-19 pandemic. There are several instances that Third-party apps would be appropriate for use during this crisis:

- Conducting briefs on COVID-related activities or assistance where the information is unclassified and not Controlled Unclassified Information
- Conducting contingency communications between commands and personnel
- Communicating with personnel that is not specifically mission-focused
- As noted in ALCOAST 096/20, telehealth use is authorized

MOBILE DEVICES:
Third-Party teleconferencing apps may be ONLY downloaded on personal mobile devices or CG GFE mobile devices, (e.g., smart phones, tablets).

IMPORTANT NOTES:

- The Centralized Support Desk (CSD) and CGFIXIT are not able to provide support for Third-party applications that are intended for off-network use. Contact those service providers directly for support.
- Keep Privacy, Operational (OPSEC), and Cybersecurity in mind at all times!

CONDITIONS OF USE:

1. If Third-party apps are procured using USCG funds, the Opt Out Requirement must be checked (Mandatory for USCG-funded accounts).
2. Users are required to opt out of the "sale" of personal data to prevent Third-party apps from sharing PII with third parties (namely advertising programs such as Google Ads and Google Analytics). Opting out is accomplished by clicking on the "Do Not 'Sell' My Personal Information" link or restricting cookie collection.
   *********If the Third-party apps do not allow users to opt out of using personal data then the Third-party apps are prohibited from use.*********

PROHIBITED USE:

- Use of screen shots, capturing video or audio, or recording any audio or video content (including the functions within Third-party apps) during use is strictly prohibited.
- Users of Third-party applications are not authorized, and are strictly prohibited, from displaying or discussing the following:
  - Conversations discussing or sharing USCG sensitive information (FOUO, Law Enforcement Sensitive, other Controlled Unclassified Information, and all levels of classified information);
  - Operational Security (OPSEC);
  - Personally Identifiable Information (PII), Sensitive PII, and Protected Health Information (PHI);
  - Health Insurance Portability and Accountability Act (HIPAA) related disclosures, except as allowed by ALCOAST 096/20 https://content.govdelivery.com/accounts/USDHSCG/bulletins/2825e73

FUNDING:
Funding of Third-party apps is at the discretion, and is the responsibility, of the requesting Command. If the Third-party app is not an approved enterprise application, then a Special Use Information Technology (SUIT) request must be submitted for tracking purposes.

HELPFUL LINKS:
Please check https://www.dcms.uscg.mil/Telework/ for the most updated list of programs and processes to obtain authorization for use.

Examples of prohibited commercial Third-Party applications on CGOne network for Coast Guard official business include Google Hangouts, Zoom, WhatsApp, Skype, and FaceTime Messenger. This is NOT an all-inclusive list. This excludes the approved Zoom for the medical community outlined in ALCOAST 096-20. Refer to https://www.dcms.uscg.mil/Telework/ for the most updated list.

1. Working from Home – includes links for VDI and VPN
2. Telework Program – includes Commandant Instruction for Telework
3. CG-6 Public Telework web page
4. USCG COVID page –FAQs for telework
5. FBI Warning on Third-Party apps page - risks & information using Third-Party apps

REFERENCE: U.S. Coast Guard Cybersecurity Manual, COMDTINST M5500.13F